G 7 3 9

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-374244
(43)Date of publication of application : 26.12.2002

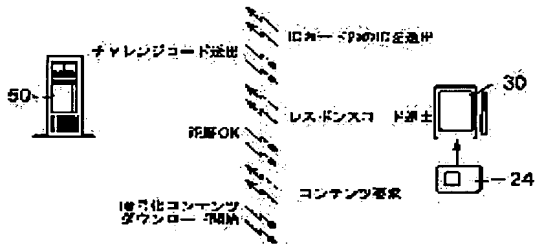
(51)Int.CI. H04L 9/32
G10K 15/02
G10L 19/00
G11B 20/10

(21)Application number : 2001-179240
(22)Date of filing : 13.06.2001

(71)Applicant : KENWOOD CORP
(72)Inventor : ISHIDA MASARU

(54) INFORMATION DISTRIBUTION METHOD

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an information distribution method, by which many unspecified terminals can download and reproduce contents, transfer the downloaded contents to other device or record the downloaded contents to other recording medium for reproduction by the other device, a diversified recording media can be used and unauthorized use of contents can be prevented fully.
SOLUTION: This method employs an IC card 24, that records an ID by each user to identify a user and a secret key by each user used, for identifying the user and for encrypting/decrypting data. A mobile phone 30, to which the IC card 24 is loaded, is connected to a server 50 via a communication line, and the server 50 authenticates the user by using the ID and the secret key in the IC card 24. When the server 50 authenticates the user, the server 50 distributes encrypted contents, by using the same secret key as that in the IC card 24 to the mobile phone 30. The distributed contents are decrypted and reproduced, by using the secret key in the IC card 24.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2002－374244
（P2002－374244A）
(43)公開日　平成14年12月26日(2002.12.26)

(51)Int.Cl.'	識別記号	FI		テーマコード'(参考)
Ｈ０４Ｌ　9/32		Ｇ１０Ｋ　15/02		５Ｄ０４４
Ｇ１０Ｋ　15/02		Ｇ１１Ｂ　20/10	Ｈ	５Ｊ１０４
Ｇ１０Ｌ　19/00		Ｈ０４Ｌ　9/00	６７５Ａ	
Ｇ１１Ｂ　20/10		Ｇ１０Ｌ　9/00	Ｎ	
		Ｈ０４Ｌ　9/00	６７３Ｅ	

審査請求　未請求　請求項の数６　ＯＬ　（全６頁）

(21)出願番号　特願2001－179240(P2001－179240)

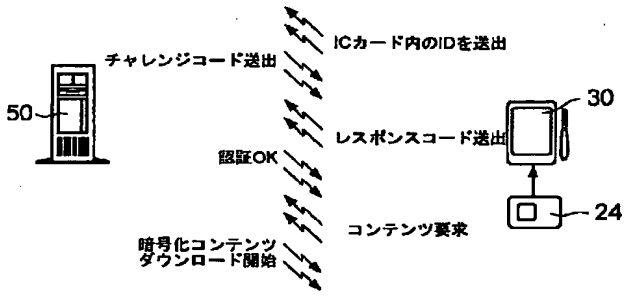
(22)出願日　平成13年６月13日(2001.6.13)

(71)出願人　000003595
株式会社ケンウッド
東京都八王子市石川町2967番地３
(72)発明者　石田　勝
東京都渋谷区道玄坂１丁目14番６号　株式会社ケンウッド内
(74)代理人　100086368
弁理士　萩原　誠

Ｆターム(参考)　5D044 AB05 AB07 BC04 CC06 DE50
GK12 GK17 HL08
5J104 AA07 AA12 KA01 KA06 NA02
NA35 NA36 NA37 NA41 PA02

(54)【発明の名称】　情報配信方法

(57)【要約】
【課題】　不特定多数の端末でコンテンツをダウンロードし再生することができ、ダウンロードされたコンテンツは他の機器に転送して、或いは他の記録媒体に記録して他の機器で再生することもでき、記録媒体は様々な記録媒体を利用でき、コンテンツの不正使用防止も充分図れる情報配信方法を提供すること。
【解決手段】　ユーザを特定するためのユーザ毎のＩＤとユーザの特定および暗復号化に使用されるユーザ毎の秘密鍵とを記録したＩＣカード２４を使用する。このＩＣカード２４を装填した移動体電話機３０を通信回線を介してサーバ５０と接続して、ＩＣカード２４内のＩＤと秘密鍵を使用してユーザの認証をサーバ５０で得る。認証が得られると、ＩＣカード２４内の秘密鍵と同一秘密鍵で暗号化されたコンテンツをサーバ５０より移動体電話機３０に配信する。配信されたコンテンツはＩＣカード２４内の秘密鍵を使用して復号化して再生される。



1

【特許請求の範囲】

【請求項１】　ユーザを特定するためのユーザ毎のＩＤとユーザの特定および暗復号化に使用されるユーザ毎の秘密鍵とを記録した情報カードと、

この情報カードを有する端末を通信回線を介してサーバと接続して、前記情報カード内のＩＤと秘密鍵を使用してユーザの認証をサーバ側で得る手段と、

この手段で認証が得られると、前記情報カード内の秘密鍵と同一秘密鍵で暗号化された情報を前記サーバより前記端末に配信し、端末の記録媒体に情報を格納する手段とを具備することを特徴とする情報配信方法。

【請求項２】　配信された前記情報を前記情報カード内の秘密鍵を使用して復号化して再生する手段が付加されたことを特徴とする請求項１に記載の情報配信方法。

【請求項３】　前記再生は、情報が配信された前記端末で行われることを特徴とする請求項２に記載の情報配信方法。

【請求項４】　前記再生は、端末に配信された情報を他の機器に転送して、あるいは他の記録媒体に記録して他の機器で行われることを特徴とする請求項２に記載の情報配信方法。

【請求項５】　前記情報カード内の前記ＩＤおよび前記秘密鍵は暗号化されていることを特徴とする請求項１ないし４のいずれかに記載の情報配信方法。

【請求項６】　前記認証は、第１に端末から情報カード内のＩＤをサーバに送出し、第２にサーバからチャレンジコードを端末に送出し、第３に端末から情報カード内の秘密鍵を使用して生成されたレスポンスコードをサーバに送出することにより行われることを特徴とする請求項１ないし５のいずれかに記載の情報配信方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、情報配信方法に関する。

【０００２】

【従来の技術】最近、パソコンや移動体電話機、あるいは携帯プレーヤなどの端末に対して通信回線を介して音楽などの情報を配信するサービスが数多く行われている。

【０００３】図６は、従来の情報配信方法を移動体電話機を例にとって説明するための図である。この図において、１１は移動体電話機、１２は配信サーバである。情報の配信を行う場合は、まず移動体電話機１１において発信動作が行われ、移動体電話機１１が通信回線を介して配信サーバ１２に接続される。すると、移動体電話機１１から端末固有の情報、例えば内部に保存されている自機の電話番号がサーバ１２に送出される。サーバ１２は、この電話番号を受信して、端末（移動体電話機１１）が情報（以下コンテンツと言う）を利用できる端末であるか否かを判断する。そして、サーバ１２において

2

移動体電話機１１がコンテンツを利用できる端末であると確認されると、サーバ１２は、移動体電話機１１に対してパスワードを要求する。この要求に対して移動体電話機１１はパスワードをサーバ１２に送出する。そして、このパスワードが正しいとサーバ１２で判断されると、サーバ１２は認証ＯＫを移動体電話機１１に通知する。すると、移動体電話機１１はコンテンツの要求をサーバ１２に送出し、サーバ１２はその要求を受けてコンテンツのダウンロード（配信）を開始する。ダウンロードされたコンテンツは、移動体電話機１１内の記録媒体に格納され、移動体電話機１１で再生できる。

【０００４】

【発明が解決しようとする課題】このように、従来は、電話番号など、端末内部に直接保存されている情報を使用して、端末がコンテンツを利用できる端末であるかを確認して、その端末に限ってコンテンツをダウンロードしている。したがって、同一ユーザでも端末を変えてコンテンツをダウンロードできないし、ダウンロードされたコンテンツを端末から他の機器に転送させることもできなかった。図７は転送の様子を示しており、コンテンツがダウンロードされた移動体電話機１１からパソコン１３にコンテンツを転送してＣＤ－Ｒ（追記型光ディスク）１４にコンテンツを書込もうとしているが、従来は不可能であった。また、従来は、ダウンロードされたコンテンツを格納する記録媒体に著作権保護機構を付ける必要があるから、利用できる記録媒体の種類が限られていた。

【０００５】本発明は上記の点に鑑みなされたもので、その目的は、不特定多数の端末でコンテンツをダウンロードし再生することができるとともに、ダウンロードされたコンテンツを他の機器に転送して、あるいは他の記録媒体に記録して他の機器で再生することもでき、さらには、コテンツを格納する記録媒体として様々な記録媒体を利用できるとともに、コンテンツの不正使用を充分防止できる情報配信方法を提供することにある。

【０００６】

【課題を解決するための手段】本発明の情報配信方法は、ユーザを特定するためのユーザ毎のＩＤとユーザの特定および暗復号化に使用されるユーザ毎の秘密鍵とを記録した情報カードと、この情報カードを有する端末を通信回線を介してサーバと接続して、前記情報カード内のＩＤと秘密鍵を使用してユーザの認証をサーバ側で得る手段と、この手段で認証が得られると、前記情報カード内の秘密鍵と同一秘密鍵で暗号化された情報を前記サーバより前記端末に配信し、端末の記録媒体に情報を格納する手段とを具備することを特徴とする。

【０００７】好ましい形態として、配信された前記情報を前記情報カード内の秘密鍵を使用して復号化して再生する手段が付加される。この手段による再生は、情報が配信された前記端末で行われる。あるいは、端末に配信

された情報を他の機器に転送して、あるいは他の記録媒体に記録して他の機器で再生が行われる。前記情報カード内の前記ＩＤおよび前記秘密鍵は暗号化されている。また、前記認証は、第１に端末から情報カード内のＩＤをサーバに送出し、第２にサーバからチャレンジコードを端末に送出し、第３に端末から情報カード内の秘密鍵を使用して生成されたレスポンスコードをサーバに送出することにより行われる。

【０００８】

【発明の実施の形態】次に添付図面を参照して本発明による情報配信方法の実施の形態を詳細に説明する。本発明の実施の形態では、ユーザを特定するためのユーザ毎のＩＤと、ユーザの特定および暗復号化に使用されるユーザ毎の秘密鍵とを記録した情報カードが使用される。この情報カードとしては具体的にはＩＣカードが使用される。ＩＣカードへのＩＤおよび秘密鍵の書込みは、配信業者にて行われる。ＩＤおよび秘密鍵は、情報の外部漏洩を防止するため暗号化されてＩＣカード内に記録される。

【０００９】図３は、ＩＣカードへのＩＤおよび秘密鍵の書込み方法を具体的に示す図である。この図において、２１はパソコン、２２はマスタ鍵保管装置、２３はＩＣカードリーダライタである。マスタ鍵保管装置２２は、マスタ鍵を保管し、各ユーザの秘密鍵を生成するときに参照される。ＩＣカードリーダライタ２３は、ＩＣカード２４のデータの読込み、書込みを行う。パソコン２１はＩＣカード書込み専用ソフトウェアを有し、ＩＤの設定、秘密鍵の生成、マスタ鍵保管装置２２およびＩＣカードリーダライタ２３の制御を行う。

【００１０】上記装置によってＩＣカード２４へＩＤおよび秘密鍵を書込む場合は、まずパソコン２１にマスタ鍵保管装置２２とＩＣカードリーダライタ２３を接続し、電源を入れる。次に、パソコン２１を起動し、ＩＣカード書込み専用ソフトウェアを起動する。次に、書込み処理初回時のみ、パソコン２１において、マスタ鍵保管装置２２内の使用するマスタ鍵を設定する。次に、パソコン２１において、ＩＣカード書込み専用ソフトウェアの画面にＩＤを設定する。その後、ＩＣカード２４をＩＣカードリーダライタ２３に挿入する。その後、パソコン２１において、ＩＣカード書込み専用ソフトウェアに書込み指示をする。すると、パソコン２１のＩＣカード書込み専用ソフトウェアの画面に設定されたＩＤがＩＣカードリーダライタ２３によってＩＣカード２４に書込まれるとともに、マスタ鍵保管装置２２内のマスタ鍵を使用してパソコン２１で生成された秘密鍵がＩＣカードリーダライタ２３によってＩＣカード２４に書込まれる。このとき、ＩＤおよび秘密鍵は暗号化されてＩＣカード２４に書込まれる。

【００１１】図４は、本発明の実施の形態でダウンロード端末として使用されるオーディオ再生機能付き移動体電話機３０の構成を示すブロック図である。この移動体電話機３０は、通信機能部３１、表示部３２、入力部３３、ＣＰＵ３４、ＩＣカード読取り部３５、メモリ３６、デコーダ部３７、アンプ部３８、およびインタフェイス部３９で構成される。

【００１２】通信機能部３１は、移動体電話機の通信部分で、基地局と通信を行う。表示部３２は、電話番号やコンテンツ情報などを表示する。入力部３３は、電話番号やコンテンツの指示などの情報を入力する。ＣＰＵ３４は、電話機の制御全般を行う。ＩＣカード読取り部３５は、図３のＩＣカード２４に記録されているＩＤおよび秘密鍵を読取る。メモリ３６は、ダウンロードしたデータ（コンテンツ）を格納する。デコーダ部３７は、ＩＣカード読取り部３５で読取られた図３のＩＣカード２４内の秘密鍵を使用してメモリ３６内のデータ（コンテンツ）を復号化する。アンプ部３８は、復号化された信号を、ヘッドホンを駆動するために増幅する。このアンプ部３８の出力にヘッドホン４０が接続される。インタフェース部３９は、電話機をパソコンなどと接続するためのインタフェイスである。

【００１３】本発明の実施の形態では、図１に示すように、ユーザ毎のＩＤと秘密鍵とが図３の装置で書込まれたＩＣカード２４を図４の移動体電話機３０に装填して、前記ＩＣカード２４内のＩＤおよび秘密鍵を使用してユーザの認証を配信サーバ５０側で行いながら、前記秘密鍵と同一秘密鍵で暗号化されたコンテンツが配信サーバ５０から移動体電話機３０に対してダウンロードされる。このダウンロードの詳細を前記図１と図２のフローチャートを参照して以下説明する。

【００１４】ダウンロードを開始する場合は、まず移動体電話機３０で発信動作が行われる。この発信動作により移動体電話機３０は通信回線に接続され（ステップＳ１）、さらに通信回線を介して配信サーバ５０に接続される（ステップＳ２）。すると、移動体電話機３０は、装填されたＩＣカード２４からＩＤを読取って（ステップＳ３）、ＩＤをサーバ５０に送出する(ステップＳ４)。サーバ５０は、送出されたＩＤを受信して、受信したＩＤによりユーザを確認し、そのユーザに対する固有のチャレンジコードを生成して、そのチャレンジコードを移動体電話機３０に送出する。

【００１５】移動体電話機３０は、チャレンジコードを受信すると（ステップＳ５）、そのチャレンジコードに対して、ＩＣカード２４内の秘密鍵を使用してレスポンスコードを生成し（ステップＳ６）、そのレスポンスコードをサーバ５０に送出する（ステップＳ７）。サーバ５０は、送出されたレスポンスコードを受信して、受信したレスポンスコードが正しいか判断し、正しければ認証ＯＫを移動体電話機３０に通知し（ステップＳ８）、動作を継続する。ここで、認証がＯＫでなかった場合は、サーバ５０は通信回線を切断し（ステップＳ１

１）、動作を終了する。

【００１６】認証がＯＫとなると(ステップＳ８)、移動体電話機３０はサーバ５０に対してコンテンツの要求を送出する(ステップＳ９)。サーバ５０は、その要求を受信すると、ＩＣカード２４に記録されている秘密鍵と同一の秘密鍵（現在のユーザの秘密鍵でサーバ５０内に保管されている）でコンテンツを暗号化して該コンテンツを移動体電話機３０にダウンロードする。すると、移動体電話機３０は、ダウンロードされた暗号化されたコンテンツを受信し(ステップＳ１０)、電話機内の図４のメモリ３６に格納する。そして、コンテンツを全て受信し終わると、移動体電話機３０は通信回線を切断し(ステップＳ１１)、動作を終了する。

【００１７】その後、図４のメモリ３６に格納されたコンテンツを読出して、ＩＣカード２４内の秘密鍵を使用して図４のデコーダ部３７でコンテンツを復号化することにより、移動体電話機３０のヘッドホン４０でコンテンツを再生できる。

【００１８】このように、上記の方法によれば、ＩＣカード２４内のＩＤおよび秘密鍵によりユーザの認証を行う。したがって、このＩＣカード２４を端末に対して着脱自在として多数の端末で使用することができるようにすることにより、不特定多数の端末でコンテンツをダウンロードすることができ、利便性が向上する。また、ダウンロードされたコンテンツはＩＣカード２４内の秘密鍵で復号化してダウンロードされた端末で再生することができるが、さらには他の機器に転送して、あるいは他の記録媒体に記録して他の機器でＩＣカード２４を使用して再生することができ、利用範囲を広げることができる。

【００１９】図５は、他の機器でコンテンツを再生する場合の具体例を示す。この具体例は、移動体電話機３０にダウンロードしたコンテンツをパソコン６１に転送してパソコン６１でＣＤ－Ｒ６２に書込み、このＣＤ－Ｒ６２を使用してカーオーディオ機器６３でコンテンツを再生する場合である。その場合は、まず、ＩＣカード２４を移動体電話機３０に装填してコンテンツを移動体電話機３０にダウンロードさせる。次に、ダウンロードしたコンテンツを移動体電話機３０からＵＳＢ経由でパソコン６１に転送する。次いで、転送したコンテンツをパソコン６１でＣＤ－Ｒドライブを使用してＣＤ－Ｒ６２に書込む。その後、ＣＤ－Ｒ６２とＩＣカード２４をカーオーディオ機器６３に移し、ＩＣカード２４内の秘密鍵でＣＤ－Ｒ６２内のコンテンツを復号化しながらカーオーディオ機器６３でコンテンツを再生する。

【００２０】このとき、ＩＣカード２４が無ければコンテンツの復号化および再生ができないため、上記のように他の記録媒体にコンテンツを書込んだり、他の機器にコンテンツを転送しても、本発明の方法によれば、コンテンツの不正使用は充分防止できる。また、コンテンツ自体が暗号化されていて、記録媒体でコンテンツの保護を図る必要がないので、本発明の方法によれば、移動体電話機内の半導体メモリやＣＤ－Ｒなど様々な記録媒体を利用できる。

【００２１】なお、コンテンツは、転送先の機器、図５ではパソコン６１でＩＣカード２４を使用して再生することもできる。また、ダウンロードし再生するコンテンツは、音楽情報や画像情報、あるいは案内情報などのどれでもよく、種類を問わない。さらに、コンテンツをダウンロードする端末も移動体電話機に限定されない。

【００２２】

【発明の効果】以上詳細に説明したように本発明の情報配信方法によれば、不特定多数の端末でコンテンツをダウンロードし再生することができるとともに、ダウンロードされたコンテンツを他の機器に転送して、あるいは他の記録媒体に記録して他の機器で再生することもでき、さらには、コテンツを格納する記録媒体として様々な記録媒体を利用できるとともに、コンテンツの不正使用を充分防止できる。

【図面の簡単な説明】

【図１】本発明による情報配信方法の実施の形態を説明するための図。

【図２】本発明による情報配信方法の実施の形態を示すフローチャート。

【図３】ＩＣカードへのＩＤおよび秘密鍵の書込み方法を具体的に示す図。

【図４】本発明の実施の形態でダウンロード端末として使用されるオーディオ再生機能付き移動体電話機の構成を示すブロック図。

【図５】ダウンロードされたコンテンツを他の機器で再生する場合の具体例を示す図。

【図６】従来の情報配信方法を移動体電話機を例にとって説明するための図。

【図７】従来技術の問題点を説明するための図。

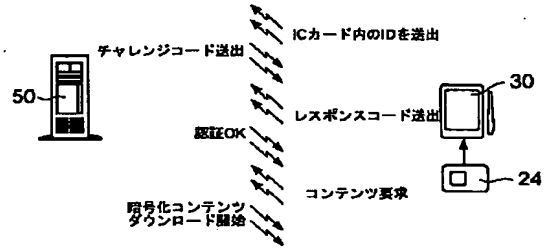
【符号の説明】

２４　ＩＣカード

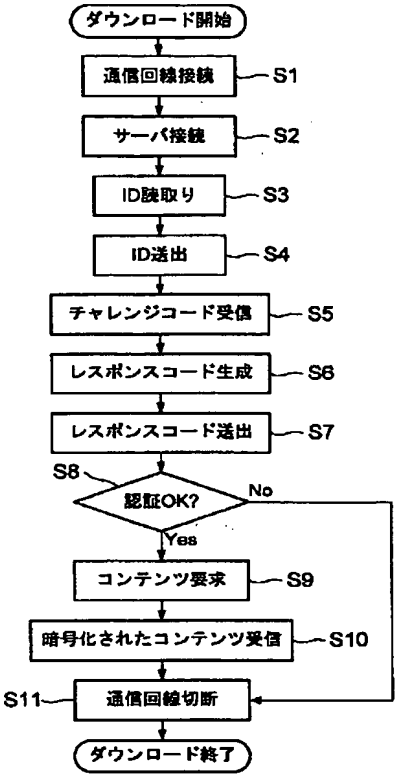
３０　移動体電話機

５０　サーバ

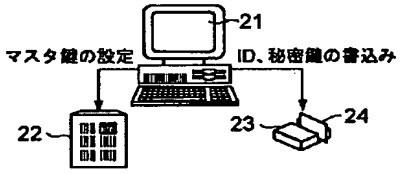
【図１】


ICカード内のIDを送出
チャレンジコード送出
50
30
レスポンスコード送出
認証OK
24
コンテンツ要求
暗号化コンテンツ
ダウンロード開始

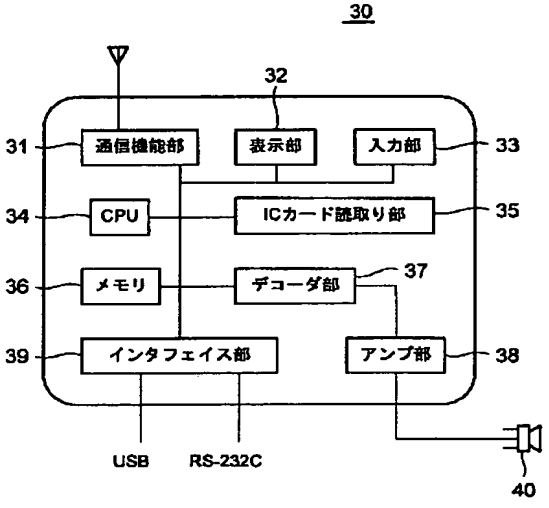
【図２】


ダウンロード開始
通信回線接続
S1
サーバ接続
S2
ID読取り
S3
ID送出
S4
チャレンジコード受信
S5
レスポンスコード生成
S6
レスポンスコード送出
S7
S8
認証OK?
No
Yes
コンテンツ要求
S9
暗号化されたコンテンツ受信
S10
S11
通信回線切断
ダウンロード終了

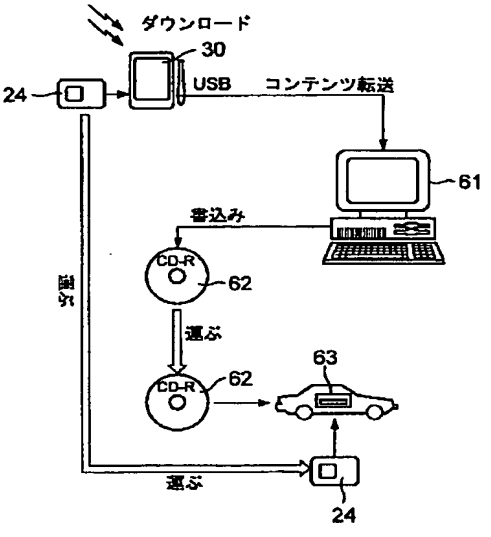
【図３】


21
マスタ鍵の設定
ID、秘密鍵の書込み
22
23
24

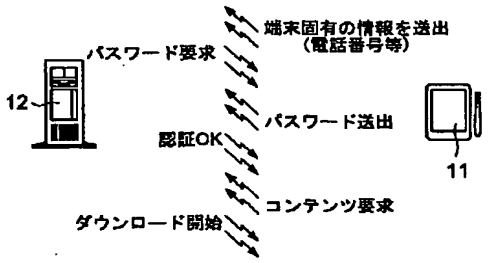
【図４】


30
32
31
通信機能部
表示部
入力部
33
34
CPU
ICカード読取り部
35
36
メモリ
デコーダ部
37
39
インタフェイス部
アンプ部
38
USB
RS-232C
40

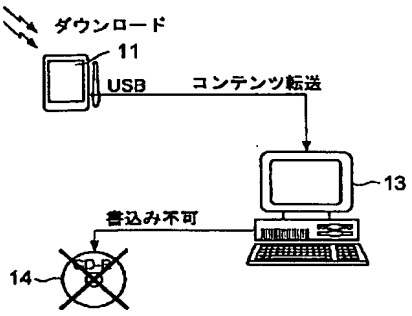
【図５】


ダウンロード
30
24
USB
コンテンツ転送
61
書込み
CD-R
62
運ぶ
63
CD-R
62
運ぶ
24

【図６】


端末固有の情報を送出
(電話番号等)
パスワード要求
12
パスワード送出
認証OK
11
コンテンツ要求
ダウンロード開始

【図７】


ダウンロード
11
USB
コンテンツ転送
13
書込み不可
14